

A characterization of $\mathbb{Z}_2\mathbb{Z}_2[u]$ -linear codes

Joaquim Borges

Received: date / Accepted: date

Abstract We prove that the class of $\mathbb{Z}_2\mathbb{Z}_2[u]$ -linear codes is exactly the class of \mathbb{Z}_2 -linear codes with automorphism group of even order. Using this characterization, we give examples of known codes, e.g. perfect codes, which has a nontrivial $\mathbb{Z}_2\mathbb{Z}_2[u]$ structure. We also exhibit an example of a \mathbb{Z}_2 -linear code which is not $\mathbb{Z}_2\mathbb{Z}_2[u]$ -linear. Also, we state that duality of $\mathbb{Z}_2\mathbb{Z}_2[u]$ -linear codes is the same that duality of \mathbb{Z}_2 -linear codes.

Finally, we prove that the class of $\mathbb{Z}_2\mathbb{Z}_4$ -linear codes which are also \mathbb{Z}_2 -linear is strictly contained in the class of $\mathbb{Z}_2\mathbb{Z}_2[u]$ -linear codes.

Keywords \mathbb{Z}_2 -linear codes, $\mathbb{Z}_2\mathbb{Z}_4$ -linear codes, $\mathbb{Z}_2\mathbb{Z}_2[u]$ -linear codes

Mathematics Subject Classification (2010) 94B60 · 94B25

1 Introduction

$\mathbb{Z}_2\mathbb{Z}_4$ -linear codes were first introduced in [13] as abelian translation-invariant propelinear codes. Later, in [4], a comprehensive description of $\mathbb{Z}_2\mathbb{Z}_4$ -linear codes appeared. In [4], the duality of such codes is studied, an appropriate inner product is defined and it is stated that the $\mathbb{Z}_2\mathbb{Z}_4$ -dual code is not the same as the standard orthogonal code, that is, using the standard inner product of binary vectors. Any $\mathbb{Z}_2\mathbb{Z}_4$ -linear code C is a binary image of a $\mathbb{Z}_2\mathbb{Z}_4$ -additive code \mathcal{C} , that is, an additive subgroup of $\mathbb{Z}_2^\alpha \times \mathbb{Z}_4^\beta$. We say that C (and also \mathcal{C}) has parameters (α, β) .

Recently, $\mathbb{Z}_2\mathbb{Z}_2[u]$ -linear codes with parameters (α, β) have been introduced in [1]. They are binary images of $\mathbb{Z}_2\mathbb{Z}_2[u]$ -additive codes, which are submodules of the ring $\mathbb{Z}_2^\alpha \times \mathbb{Z}_2[u]^\beta$. These codes have some similarities with $\mathbb{Z}_2\mathbb{Z}_4$ -linear

This work has been partially supported by the Spanish MINECO grants TIN2016-77918-P and MTM2015-69138-REDT, and by the Catalan AGAUR grant 2014SGR-691.

Joaquim Borges is with the Dept. of Information and Communications Engineering, Universitat Autònoma de Barcelona, Spain. E-mail: jborges@deic.uab.cat

codes. However, there is a key difference: every $\mathbb{Z}_2\mathbb{Z}_2[u]$ -linear code is also \mathbb{Z}_2 -linear, which is not true, in general, for $\mathbb{Z}_2\mathbb{Z}_4$ -linear codes.

The aim of this paper is to clarify the relation among all these classes. Specifically, we prove that a \mathbb{Z}_2 -linear code is $\mathbb{Z}_2\mathbb{Z}_2[u]$ -linear if and only if its automorphism group has even order. We also show that for a $\mathbb{Z}_2\mathbb{Z}_2[u]$ -linear code, its $\mathbb{Z}_2\mathbb{Z}_2[u]$ -dual code is exactly its \mathbb{Z}_2 -dual code, that is, its standard binary dual code. This, in turn, implies directly that the dual weight distributions are related by MacWilliams identity. This fact was proved in [1]. By using these properties, we find $\mathbb{Z}_2\mathbb{Z}_2[u]$ structures for all binary linear perfect codes. In particular, for any binary linear perfect code C , we compute the possible values of α and β such that C is a $\mathbb{Z}_2\mathbb{Z}_2[u]$ -linear code with parameters (α, β) .

If C is a $\mathbb{Z}_2\mathbb{Z}_4$ -linear code with parameters (α, β) , which is also \mathbb{Z}_2 -linear, then we prove that C has a $\mathbb{Z}_2\mathbb{Z}_2[u]$ structure with the same parameters (α, β) . In addition, we give an example showing that there are $\mathbb{Z}_2\mathbb{Z}_2[u]$ -linear codes which are not $\mathbb{Z}_2\mathbb{Z}_4$ -linear.

The paper is organized as follows. In the next section, we give basic definitions and concepts. In Section 3, we prove that for a given $\mathbb{Z}_2\mathbb{Z}_2[u]$ -linear code C , its $\mathbb{Z}_2\mathbb{Z}_2[u]$ -dual code is exactly C^\perp , i.e. the standard binary orthogonal code. In Section 4, we study the conditions for a \mathbb{Z}_2 -linear code to be $\mathbb{Z}_2\mathbb{Z}_2[u]$ -linear. Moreover, we characterize $\mathbb{Z}_2\mathbb{Z}_2[u]$ -linear codes as \mathbb{Z}_2 -linear codes with automorphism group of even order. In Section 5, we prove that all \mathbb{Z}_2 -linear perfect codes are $\mathbb{Z}_2\mathbb{Z}_2[u]$ -linear with parameters (α, β) , where $\beta > 0$. In addition, we compute the possible values of α and β . In Section 6, we analyze the relation to $\mathbb{Z}_2\mathbb{Z}_4$ -linear codes. In particular, we prove that if C is \mathbb{Z}_2 -linear and $\mathbb{Z}_2\mathbb{Z}_4$ -linear with parameters (α, β) , then C is also a $\mathbb{Z}_2\mathbb{Z}_2[u]$ -linear code with the same parameters (α, β) . We note that the reciprocal statement is not true. Finally, in Section 7, we give some conclusions about the meaningful of $\mathbb{Z}_2\mathbb{Z}_2[u]$ -linear codes and we point out some possible further research on the topic.

2 Preliminaries

Denote by \mathbb{Z}_2 and \mathbb{Z}_4 the rings of integers modulo 2 and modulo 4, respectively. A binary code of length n is any non-empty subset C of \mathbb{Z}_2^n . If that subset is a vector space then we say that it is a \mathbb{Z}_2 -linear code (or binary linear code).

For any binary code C , an automorphism of C is a coordinate permutation that leaves C invariant. The automorphism group of C , denoted $Aut(C)$, is the group of all automorphisms of C .

Any non-empty subset \mathcal{C} of \mathbb{Z}_4^n is a quaternary code of length n , and an additive subgroup of \mathbb{Z}_4^n is called a quaternary linear code. The elements of a code are called codewords.

The classical Gray map $\phi : \mathbb{Z}_4 \rightarrow \mathbb{Z}_2^2$ is defined by

$$\phi(0) = (0, 0), \quad \phi(1) = (0, 1), \quad \phi(2) = (1, 1), \quad \phi(3) = (1, 0).$$

If $a = (a_1, \dots, a_m) \in \mathbb{Z}_4^m$, then the Gray map of a is the coordinate-wise extended map $\phi(a) = (\phi(a_1), \dots, \phi(a_m))$. We naturally extend the Gray map for vectors $\mathbf{u} = (u \mid u') \in \mathbb{Z}_2^\alpha \times \mathbb{Z}_4^\beta$ so that $\Phi(\mathbf{u}) = (u \mid \phi(u'))$.

Definition 1 A $\mathbb{Z}_2\mathbb{Z}_4$ -additive code \mathcal{C} with parameters (α, β) is an additive subgroup of $\mathbb{Z}_2^\alpha \times \mathbb{Z}_4^\beta$.

Such codes are extensively studied in [4]. Alternatively, we can define a $\mathbb{Z}_2\mathbb{Z}_4$ -additive code as a \mathbb{Z}_4 -submodule of $\mathbb{Z}_2^\alpha \times \mathbb{Z}_4^\beta$, where the scalar product $\lambda \mathbf{x}$ is defined as $\mathbf{x} + \dots + \mathbf{x}$, λ times (of course, if $\lambda = 0$, then $\lambda \mathbf{x} = 0$), for $\lambda \in \mathbb{Z}_4$, $\mathbf{x} \in \mathbb{Z}_2^\alpha \times \mathbb{Z}_4^\beta$.

If \mathcal{C} is a $\mathbb{Z}_2\mathbb{Z}_4$ -additive code with parameters (α, β) , then the binary image $C = \Phi(\mathcal{C})$ is called a $\mathbb{Z}_2\mathbb{Z}_4$ -linear code with parameters (α, β) . Note that C is a binary code of length $n = \alpha + 2\beta$, but C is not \mathbb{Z}_2 -linear, in general [4]. If $\alpha = 0$, then C is called a \mathbb{Z}_4 -linear code. If $\beta = 0$, then C is simply a \mathbb{Z}_2 -linear code.

The standard inner product in $\mathbb{Z}_2^\alpha \times \mathbb{Z}_4^\beta$, defined in [4], can be written as

$$\mathbf{u} \cdot \mathbf{v} = 2 \left(\sum_{i=1}^{\alpha} u_i v_i \right) + \sum_{j=1}^{\beta} u'_j v'_j \in \mathbb{Z}_4,$$

where the computations are made taking the zeros and ones in the α binary coordinates as quaternary zeros and ones, respectively. The $\mathbb{Z}_2\mathbb{Z}_4$ -dual code of a $\mathbb{Z}_2\mathbb{Z}_4$ -additive code \mathcal{C} is defined in the standard way by

$$\mathcal{C}^\perp = \{ \mathbf{v} \in \mathbb{Z}_2^\alpha \times \mathbb{Z}_4^\beta \mid \mathbf{u} \cdot \mathbf{v} = 0, \text{ for all } \mathbf{u} \in \mathcal{C} \}.$$

Consider the ring $\mathbb{Z}_2[u] = \mathbb{Z}_2 + u\mathbb{Z}_2 = \{0, 1, u, 1+u\}$, where $u^2 = 0$. Note that $(\mathbb{Z}_2[u], +)$ is group-isomorphic to the Klein group $(\mathbb{Z}_2^2, +)$. But with the product operation, $(\mathbb{Z}_2[u], \cdot)$ is monoid-isomorphic to (\mathbb{Z}_4, \cdot) . Define the map $\pi : \mathbb{Z}_2[u] \rightarrow \mathbb{Z}_2$, such that $\pi(0) = \pi(u) = 0$ and $\pi(1) = \pi(1+u) = 1$. Then, for $\lambda \in \mathbb{Z}_2[u]$ and $\mathbf{x} = (x_1, \dots, x_\alpha \mid x'_1, \dots, x'_\beta) \in \mathbb{Z}_2^\alpha \times \mathbb{Z}_2[u]^\beta$, we can consider the scalar product

$$\lambda \mathbf{x} = (\pi(\lambda)x_1, \dots, \pi(\lambda)x_\alpha \mid \lambda x'_1, \dots, \lambda x'_\beta) \in \mathbb{Z}_2^\alpha \times \mathbb{Z}_2[u]^\beta.$$

With this operation, $\mathbb{Z}_2^\alpha \times \mathbb{Z}_2[u]^\beta$ is a $\mathbb{Z}_2[u]$ -module. Note that, a $\mathbb{Z}_2[u]$ -submodule of $\mathbb{Z}_2^\alpha \times \mathbb{Z}_2[u]^\beta$ is not the same as a subgroup of $\mathbb{Z}_2^\alpha \times \mathbb{Z}_2[u]^\beta$.

Definition 2 ([1]) A $\mathbb{Z}_2\mathbb{Z}_2[u]$ -additive code \mathcal{C} with parameters (α, β) is a $\mathbb{Z}_2[u]$ -submodule of $\mathbb{Z}_2^\alpha \times \mathbb{Z}_2[u]^\beta$.

The following straightforward equivalence can be used as an alternative definition.

Lemma 1 A code $\mathcal{C} \subseteq \mathbb{Z}_2^\alpha \times \mathbb{Z}_2[u]^\beta$ is $\mathbb{Z}_2\mathbb{Z}_2[u]$ -additive if and only if

$$\begin{aligned} u\mathbf{z} &\in \mathcal{C} \quad \forall \mathbf{z} \in \mathcal{C}, \text{ and} \\ \mathbf{x} + \mathbf{y} &\in \mathcal{C} \quad \forall \mathbf{x}, \mathbf{y} \in \mathcal{C}. \end{aligned}$$

As for $\mathbb{Z}_2^\alpha \times \mathbb{Z}_4^\beta$, we can also define a Gray-like map. Let $\psi : \mathbb{Z}_2[u] \rightarrow \mathbb{Z}_2^2$ be defined as

$$\psi(0) = (0, 0), \quad \psi(1) = (0, 1), \quad \psi(u) = (1, 1), \quad \psi(1+u) = (1, 0).$$

If $a = (a_1, \dots, a_m) \in \mathbb{Z}_2[u]^m$, then the coordinate-wise extension of ψ is $\psi(a) = (\psi(a_1), \dots, \psi(a_m))$. Now, we define the Gray-like map for elements $\mathbf{u} = (u \mid u') \in \mathbb{Z}_2^\alpha \times \mathbb{Z}_2[u]^\beta$ so that $\Psi(\mathbf{u}) = (u \mid \psi(u'))$.

If \mathcal{C} is a $\mathbb{Z}_2\mathbb{Z}_2[u]$ -additive code with parameters (α, β) , then the binary image $C = \Psi(\mathcal{C})$ is called a $\mathbb{Z}_2\mathbb{Z}_2[u]$ -linear code with parameters (α, β) . Note that, unlike for $\mathbb{Z}_2\mathbb{Z}_4$ -linear codes, C is a \mathbb{Z}_2 -linear code of length $n = \alpha + 2\beta$. This fact is clear since for any pair of elements $\mathbf{x}, \mathbf{y} \in \mathbb{Z}_2^\alpha \times \mathbb{Z}_2[u]^\beta$, we have that $\Psi(\mathbf{x}) + \Psi(\mathbf{y}) = \Psi(\mathbf{x} + \mathbf{y})$.

The inner product in $\mathbb{Z}_2^\alpha \times \mathbb{Z}_2[u]^\beta$, defined in [1], can be written as

$$\mathbf{u} \cdot \mathbf{v} = u \left(\sum_{i=1}^{\alpha} u_i v_i \right) + \sum_{j=1}^{\beta} u'_j v'_j \in \mathbb{Z}_2[u],$$

where the computations are made taking the zeros and ones in the α binary coordinates as zeros and ones in $\mathbb{Z}_2[u]$, respectively. The $\mathbb{Z}_2\mathbb{Z}_2[u]$ -dual code of a $\mathbb{Z}_2\mathbb{Z}_2[u]$ -additive code \mathcal{C} is defined in the standard way by

$$\mathcal{C}^\perp = \{\mathbf{v} \in \mathbb{Z}_2^\alpha \times \mathbb{Z}_2[u]^\beta \mid \mathbf{u} \cdot \mathbf{v} = 0, \text{ for all } \mathbf{u} \in \mathcal{C}\}.$$

3 Duality of $\mathbb{Z}_2\mathbb{Z}_2[u]$ -linear codes

It is readily verified that if $a, b \in \mathbb{Z}_2[u]$, then $\psi(a) \cdot \psi(b) = 1$ if and only if $ab \in \{1, u\}$. This property can be easily generalized for elements in $\mathbb{Z}_2[u]^\beta$.

Lemma 2 *If $x', y' \in \mathbb{Z}_2[u]^\beta$, then $\psi(x') \cdot \psi(y') = 1$ if and only if $x' \cdot y' \in \{1, u\}$.*

Proof Each pair of equal addends in $x' \cdot y'$ gives 0. Thus, we can omit all these pairs. The set of nonzero remaining terms is:

- (i) $\{1, u, 1+u\}$ or \emptyset , if $x' \cdot y' = 0$.
- (ii) $\{1\}$ or $\{u, 1+u\}$, if $x' \cdot y' = 1$.
- (iii) $\{u\}$ or $\{1, 1+u\}$, if $x' \cdot y' = u$.
- (iv) $\{1+u\}$ or $\{1, u\}$, if $x' \cdot y' = 1+u$.

Clearly, cases (i) and (iv) give $\psi(x') \cdot \psi(y') = 0$, whereas cases (ii) and (iii) give $\psi(x') \cdot \psi(y') = 1$.

Proposition 1 *Let $\mathbf{x}, \mathbf{y} \in \mathbb{Z}_2^\alpha \times \mathbb{Z}_2[u]^\beta$.*

- (i) *If $\mathbf{x} \cdot \mathbf{y} = 0$, then $\Psi(\mathbf{x}) \cdot \Psi(\mathbf{y}) = 0$.*
- (ii) *If $\mathbf{x} \cdot \mathbf{y} \neq 0$ and $\Psi(\mathbf{x}) \cdot \Psi(\mathbf{y}) = 0$, then $\Psi(\mathbf{x}) \cdot \Psi((1+u)\mathbf{y}) = 1$.*

Proof: Let $\mathbf{x} = (x \mid x')$ and $\mathbf{y} = (y \mid y')$. We can write the inner product of \mathbf{x} and \mathbf{y} as $\mathbf{x} \cdot \mathbf{y} = u(x \cdot y) + (x' \cdot y')$.

- (i) If $\mathbf{x} \cdot \mathbf{y} = 0$, then either (a) $x \cdot y = x' \cdot y' = 0$, or (b) $x \cdot y = 1$ and $x' \cdot y' = u$.
 - (a) By Lemma 2, we have that $\Psi(x') \cdot \Psi(y') = 0$ and hence $\Psi(\mathbf{x}) \cdot \Psi(\mathbf{y}) = 0$.
 - (b) Again, By Lemma 2, we obtain $\Psi(x') \cdot \Psi(y') = 1$ and then $\Psi(\mathbf{x}) \cdot \Psi(\mathbf{y}) = 0$.
- (ii) If $\mathbf{x} \cdot \mathbf{y} \neq 0$, then either (a) $x \cdot y = 0$ and $x' \cdot y' \neq 0$, or (b) $x \cdot y = 1$ and $x' \cdot y' \neq u$.
 - (a) In this case $x' \cdot y' \in \{1, u, 1+u\}$. But $x \cdot y = 0$ and $\Psi(\mathbf{x}) \cdot \Psi(\mathbf{y}) = 0$ imply that $\Psi(x') \cdot \Psi(y') = 0$ and hence, by Lemma 2, the only possible case is that $x' \cdot y' = 1+u$. Therefore, $x' \cdot ((1+u)y') = 1$ and $\Psi(x') \cdot \Psi((1+u)y') = 1$, again by Lemma 2. Thus, $\Psi(\mathbf{x}) \cdot \Psi((1+u)\mathbf{y}) = 1$.
 - (b) We have $x' \cdot y' \in \{0, 1, 1+u\}$. Since $x \cdot y = 1$ and $\Psi(\mathbf{x}) \cdot \Psi(\mathbf{y}) = 0$, we obtain $\Psi(x') \cdot \Psi(y') = 1$. By Lemma 2, the only possibility is $x' \cdot y' = 1$. Hence, $x' \cdot ((1+u)y') = 1+u$ and $\Psi(x') \cdot \Psi((1+u)y') = 0$. We conclude $\Psi(\mathbf{x}) \cdot \Psi((1+u)\mathbf{y}) = 1$.

□

Corollary 1 *Let \mathcal{C} be a $\mathbb{Z}_2\mathbb{Z}_2[u]$ -additive code and let $C = \Psi(\mathcal{C})$ be the corresponding binary $\mathbb{Z}_2\mathbb{Z}_2[u]$ -linear code. Then, $\Psi(\mathcal{C}^\perp) = C^\perp$.*

Proof: If $\mathbf{x} \in \mathcal{C}^\perp$, then $\mathbf{x} \cdot \mathbf{c} = 0$, for all $\mathbf{c} \in \mathcal{C}$. Hence, by Proposition 1(i), we have that $\Psi(\mathbf{x}) \cdot \Psi(\mathbf{c}) = 0$, for all $\mathbf{c} \in \mathcal{C}$, implying that $\Psi(\mathbf{x}) \in C^\perp$. We have proved $\Psi(\mathcal{C}^\perp) \subseteq C^\perp$.

If $\mathbf{x} \notin \mathcal{C}^\perp$, then $\mathbf{x} \cdot \mathbf{c} \neq 0$, for some $\mathbf{c} \in \mathcal{C}$. Now, by Proposition 1(ii), we have that $\Psi(\mathbf{x}) \cdot \Psi(\mathbf{c}) \neq 0$ or $\Psi(\mathbf{x}) \cdot \Psi((1+u)\mathbf{c}) \neq 0$. It follows that $\Psi(\mathbf{x}) \notin C^\perp$ and therefore $C^\perp \subseteq \Psi(\mathcal{C}^\perp)$. □

Obviously, this immediately implies that the weight distributions of \mathcal{C} and C^\perp are related by MacWilliams identity, as it was proved in [1].

To finish this section, we prove that the dual of a $\mathbb{Z}_2\mathbb{Z}_2[u]$ -linear code is also $\mathbb{Z}_2\mathbb{Z}_2[u]$ -linear with the same parameters.

Proposition 2 *A binary code C is $\mathbb{Z}_2\mathbb{Z}_2[u]$ -linear with parameters (α, β) if and only if C^\perp is $\mathbb{Z}_2\mathbb{Z}_2[u]$ -linear with the same parameters (α, β) .*

Proof: Since $(C^\perp)^\perp = C$, it is enough to prove the ‘only if’ part. Assume that C is a $\mathbb{Z}_2\mathbb{Z}_2[u]$ -linear code with parameters (α, β) . Let $C^\perp = \Psi^{-1}(C^\perp)$. By linearity of C^\perp and Lemma 1, we only need to proof that $u\Psi^{-1}(c) \in C^\perp$, for all $c \in C^\perp$. For any codeword $\mathbf{x} \in \mathcal{C}$, we have $(u\Psi^{-1}(c)) \cdot \mathbf{x} = u(\Psi^{-1}(c) \cdot \mathbf{x}) = u0 = 0$, which implies $u\Psi^{-1}(c) \in C^\perp$. □

4 Characterization of $\mathbb{Z}_2\mathbb{Z}_2[u]$ -linear codes

Given a \mathbb{Z}_2 -linear code C of length n , a natural question is if we can choose a set of β pairs of coordinates such that C is a $\mathbb{Z}_2\mathbb{Z}_2[u]$ -linear code with parameters $(n-2\beta, \beta)$. The next lemma shows us that it is enough to answer the question for a generator matrix of C .

As it is pointed out in [12, Problem (32), p. 230], $\text{Aut}(C)$ is trivial, i.e. it only contains the identity permutation. Therefore, C is not $\mathbb{Z}_2\mathbb{Z}_2[u]$ -linear for $\beta > 0$.

In the next section we see several examples of well-known codes with a $\mathbb{Z}_2\mathbb{Z}_2[u]$ structure.

5 $\mathbb{Z}_2\mathbb{Z}_2[u]$ -linear perfect codes

A binary *repetition* code $C = \{(0, \dots, 0), (1, \dots, 1)\}$ of odd length n is a trivial perfect code. Its dual code is the *even* code which contains all vectors of length n and even weight (i.e. with an even number of nonzero coordinates). Clearly, these codes can be considered as $\mathbb{Z}_2\mathbb{Z}_2[u]$ -linear codes with parameters $(n - 2\beta, \beta)$, for all $\beta \in \{0, \dots, (n-1)/2\}$.

It is well known that the binary linear perfect codes with more than two codewords are:

- (1) The binary *Hamming* 1-perfect codes of length $n = 2^t - 1$ ($t \geq 3$), dimension $k = 2^t - t - 1$ and minimum distance $d = 3$.
- (2) The binary *Golay* 3-perfect code of length $n = 23$, dimension $k = 12$ and minimum distance $d = 7$.

In this section we prove that these codes are $\mathbb{Z}_2\mathbb{Z}_2[u]$ -linear codes.

Let H_t be a Hamming code of length $n = 2^t - 1$, where $t \geq 3$. The dual code H_t^\perp is known as the *simplex* code. It is a constant-weight code with all nonzero codewords of weight 2^{t-1} . A parity-check matrix M_r for H_t (which is a generator matrix for H_t^\perp) contains all nonzero column vectors of length t .

Theorem 1 *Let H_t be a Hamming code of length $n = 2^t - 1$. Then, H_t is a $\mathbb{Z}_2\mathbb{Z}_2[u]$ -linear code with parameters $(2^r - 1, 2^{t-1} - 2^{r-1})$, for all r such that $t/2 \leq r \leq t$.*

Proof The case $r = t$ corresponds to the trivial case $(\alpha, \beta) = (n, 0)$. In [8], it is shown that $\text{Aut}(H_t)$ contains involutions fixing $2^r - 1$ points for $t/2 \leq r \leq t$. Thus, the statement follows by Proposition 3.

Example 2 A parity-check matrix for H_3 is

$$M_3 = \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix}.$$

We can take the pairs of coordinates $(4, 5)$ and $(6, 7)$ as $\mathbb{Z}_2[u]$ coordinates and consider the $\mathbb{Z}_2\mathbb{Z}_2[u]$ -additive code \mathcal{C} generated by

$$\begin{pmatrix} 0 & 0 & 0 & u & u \\ 0 & 1 & 1 & 0 & u \\ 1 & 0 & 1 & 1 & 1 \end{pmatrix}.$$

Note that multiplying u by any row gives the allzero vector or a weight 4 vector whose binary image is in H_3^\perp . Thus, $\Psi(\mathcal{C}) = H_3^\perp$. Hence, by Corollary 1 and Proposition 2, H_3 is a $\mathbb{Z}_2\mathbb{Z}_2[u]$ -linear code with parameters $(3, 2)$. We remark that H_3 is also a $\mathbb{Z}_2\mathbb{Z}_4$ -linear code with the same parameters. But, according to [6], H_t is not $\mathbb{Z}_2\mathbb{Z}_4$ -linear for $\beta > 0$ and $t > 3$.

Example 3 Consider the parity-check matrix for H_4

$$M_4 = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}.$$

Again, we can take the pairs of coordinates $(8, 9)$, $(10, 11)$, $(12, 13)$ and $(14, 15)$ as $\mathbb{Z}_2[u]$ coordinates. Let \mathcal{C} be the $\mathbb{Z}_2\mathbb{Z}_2[u]$ -additive code generated by

$$\begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & u & u & u & u \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & u & 0 & u \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & u & u \end{pmatrix}.$$

Multiplying any row by u gives the allzero vector or a weight 8 vector whose binary image is in H_4^\perp . Therefore, $\Psi(\mathcal{C}) = H_4^\perp$ and H_4 is a $\mathbb{Z}_2\mathbb{Z}_2[u]$ -linear code with parameters $(7, 4)$. Note that, taking the same pairs of coordinates as quaternary coordinates, it is also true that H_4^\perp is a $\mathbb{Z}_2\mathbb{Z}_4$ -linear code, but the $\mathbb{Z}_2\mathbb{Z}_4$ -dual code is not a Hamming code. For example, the vector $v = (0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1)$ is not orthogonal to the third row of M_4 . However, v is in the $\mathbb{Z}_2\mathbb{Z}_4$ -dual of H_4^\perp .

After a permutation of columns, the matrix M_4 can be written as

$$\begin{pmatrix} 1 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 1 \\ 1 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 0 \end{pmatrix}.$$

Now, taking the pairs of coordinates $(i, i + 1)$ for $i = 4, \dots, 14$ as $\mathbb{Z}_2[u]$ coordinates, we also have that H_4^\perp is the binary image of the code generated by

$$\begin{pmatrix} 1 & 1 & 0 & 1 & 1 & u & 1 + u & 1 & 0 \\ 0 & 1 & 1 & 0 & 1 & 1 & u & 1 + u & 1 \\ 1 & 1 & 0 & 1 + u & 1 + u & u & 1 & 1 + u & 0 \\ 1 & 0 & 1 & 0 & 1 + u & 1 & u & 1 & 1 + u \end{pmatrix}.$$

Therefore, H_4 is also a $\mathbb{Z}_2\mathbb{Z}_2[u]$ -linear code with parameters $(3, 6)$.

Corollary 3 *The extended Hamming code H_t' , the dual of a Hamming code H_t^\perp (simplex code), and the dual of an extended Hamming code $(H_t')^\perp$ (linear Hadamard code) are $\mathbb{Z}_2\mathbb{Z}_2[u]$ -linear codes with parameters $(2^r, 2^{t-1} - 2^{r-1})$, $(2^r - 1, 2^{t-1} - 2^{r-1})$, and $(2^r, 2^{t-1} - 2^{r-1})$, respectively.*

Proof: On the one hand, extending a $\mathbb{Z}_2\mathbb{Z}_2[u]$ -linear code with parameters (α, β) trivially results in a $\mathbb{Z}_2\mathbb{Z}_2[u]$ -linear code with parameters $(\alpha + 1, \beta)$. On the other hand, by Proposition 2, the dual code has the same parameters. \square

Theorem 2 *The binary Golay code G_{23} and the extended binary Golay code G_{24} are $\mathbb{Z}_2\mathbb{Z}_2[u]$ -linear codes with parameters (α, β) . For $\beta > 0$, the parameters are:*

- (i) $(0, 12)$ or $(8, 8)$, for G_{24} .
- (ii) $(7, 8)$, for G_{23} .

Proof: It is well known that the automorphism groups of G_{23} and G_{24} are the Mathieu groups M_{23} and M_{24} , respectively [12]. In [10], it is stated that M_{24} has 43470 fixed-point-free involutions. The remaining involutions of M_{24} are 11385 involutions fixing 8 points. Therefore, by Proposition 3, G_{24} has 43470 $\mathbb{Z}_2\mathbb{Z}_2[u]$ different structures with parameters $(0, 12)$ and 11385 with parameters $(8, 8)$. For the case of M_{23} , it has 3795 involutions, all of them fixing 7 points. Therefore, G_{23} has 3795 $\mathbb{Z}_2\mathbb{Z}_2[u]$ structures with parameters $(7, 8)$. \square

6 $\mathbb{Z}_2\mathbb{Z}_2[u]$ -linear and $\mathbb{Z}_2\mathbb{Z}_4$ -linear codes

In this section we prove that any $\mathbb{Z}_2\mathbb{Z}_4$ -linear code with parameters (α, β) which is also \mathbb{Z}_2 -linear has a $\mathbb{Z}_2\mathbb{Z}_2[u]$ structure with the same parameters. It is not difficult to see this property using Corollary 2, however, we give here an independent proof in order to better clarify the relation between both classes of codes.

The following property was stated in [11] for vectors over \mathbb{Z}_4 . Its generalization for vectors over $\mathbb{Z}_2 \times \mathbb{Z}_4$ is easy and established in [9].

Lemma 4 *Let $\mathbf{x}, \mathbf{y} \in \mathbb{Z}_2^\alpha \times \mathbb{Z}_4^\beta$. The following identity holds:*

$$\Phi(\mathbf{x}) + \Phi(\mathbf{y}) = \Phi(\mathbf{x} + \mathbf{y}) + \Phi(2(\mathbf{x} \star \mathbf{y})),$$

where \star stands for the coordinate-wise product.

The next lemma [9] is a direct consequence.

Lemma 5 *If \mathcal{C} is a $\mathbb{Z}_2\mathbb{Z}_4$ -additive code, then its binary image $C = \Phi(\mathcal{C})$ is \mathbb{Z}_2 -linear if and only if $2(\mathbf{x} \star \mathbf{y}) \in \mathcal{C}$, for all $\mathbf{x}, \mathbf{y} \in \mathcal{C}$.*

Define the map $\theta : \mathbb{Z}_2^\alpha \times \mathbb{Z}_4^\beta \longrightarrow \mathbb{Z}_2^\alpha \times \mathbb{Z}_2[u]^\beta$ such that, for every element $(x_1, \dots, x_\alpha \mid y_1, \dots, y_\beta) \in \mathbb{Z}_2^\alpha \times \mathbb{Z}_4^\beta$,

$$\theta(x_1, \dots, x_\alpha \mid y_1, \dots, y_\beta) = (x_1, \dots, x_\alpha \mid \vartheta(y_1), \dots, \vartheta(y_\beta)),$$

where $\vartheta(0) = 0$; $\vartheta(1) = 1$; $\vartheta(2) = u$; $\vartheta(3) = 1 + u$. Note that $\theta = \Psi^{-1}\Phi$.

Theorem 3 *If $\mathcal{C} \subseteq \mathbb{Z}_2^\alpha \times \mathbb{Z}_4^\beta$ is a $\mathbb{Z}_2\mathbb{Z}_4$ -additive code such that $\Phi(\mathcal{C})$ is \mathbb{Z}_2 -linear, then $\mathcal{C}' = \theta(\mathcal{C}) \subseteq \mathbb{Z}_2^\alpha \times \mathbb{Z}_2[u]^\beta$ is a $\mathbb{Z}_2\mathbb{Z}_2[u]$ -additive code.*

Proof: We use the characterization of Lemma 1 to prove the statement.

Given $\mathbf{x} \in \mathcal{C}'$, we need to prove that $u\mathbf{x} \in \mathcal{C}'$. Note that $u\mathbf{x} = \theta(2\theta^{-1}(\mathbf{x}))$ which is in \mathcal{C}' .

Next, we want to prove that $\mathbf{x} + \mathbf{y} \in \mathcal{C}'$, for all $\mathbf{x}, \mathbf{y} \in \mathcal{C}'$. Clearly,

$$\mathbf{x} + \mathbf{y} = \Psi^{-1}(\Psi(\mathbf{x}) + \Psi(\mathbf{y})). \quad (1)$$

By Lemma 4, we have

$$\Psi(\mathbf{x}) + \Psi(\mathbf{y}) = \Phi(\Phi^{-1}(\Psi(\mathbf{x})) + \Phi^{-1}(\Psi(\mathbf{y})) + 2(\Phi^{-1}(\Psi(\mathbf{x})) \star \Phi^{-1}(\Psi(\mathbf{y}))))). \quad (2)$$

Combining Equations 1 and 2, we obtain

$$\mathbf{x} + \mathbf{y} = \theta(\theta^{-1}(\mathbf{x}) + \theta^{-1}(\mathbf{y}) + 2(\theta^{-1}(\mathbf{x}) \star \theta^{-1}(\mathbf{y}))).$$

Since $\Phi(\mathcal{C})$ is \mathbb{Z}_2 -linear, we have that $2(\theta^{-1}(\mathbf{x}) \star \theta^{-1}(\mathbf{y})) \in \mathcal{C}$, by Lemma 5. It follows that $\mathbf{x} + \mathbf{y} \in \mathcal{C}'$. \square

However, there are $\mathbb{Z}_2\mathbb{Z}_2[u]$ -linear codes which are not $\mathbb{Z}_2\mathbb{Z}_4$ -linear, as we can see in the following example.

Example 4 Let $\mathcal{D} \subset \mathbb{Z}_2[u]^4$ be the code generated by $\mathbf{x} = (1, 1, 1, u)$ and $\mathbf{y} = (1, u, 1, 1)$. We can see that

$$\theta(\theta^{-1}(\mathbf{x}) + \theta^{-1}(\mathbf{y})) = \theta(2, 3, 2, 3) = (u, 1 + u, u, 1 + u).$$

It is easy to check that the equation $\lambda\mathbf{x} + \mu\mathbf{y} = (u, 1 + u, u, 1 + u)$ has no solution for $\lambda, \mu \in \mathbb{Z}_2[u]$. Therefore $\mathcal{C} = \theta^{-1}(\mathcal{D})$ is not a $\mathbb{Z}_2\mathbb{Z}_4$ -additive code.

It is worth noting that if \mathcal{C} is a $\mathbb{Z}_2\mathbb{Z}_4$ -additive code such that $\Phi(\mathcal{C})$ is \mathbb{Z}_2 -linear, it is not yet true that $\Phi(\mathcal{C}^\perp) = \Phi(\mathcal{C})^\perp$ as we can see in the next example.

Example 5 Let $\mathcal{C} \subset \mathbb{Z}_4^3$ be the code generated by $\mathbf{x} = (1, 1, 1)$ and $\mathbf{y} = (0, 2, 3)$. It can be easily verified that $\Phi(\mathcal{C})$ is \mathbb{Z}_2 -linear. However, we have that $(1, 1, 2) \in \mathcal{C}^\perp$, but $\Phi(1, 1, 2) = (0, 1, 0, 1, 1, 1) \notin \Phi(\mathcal{C})^\perp$.

7 Conclusions

From Corollary 2, it seems that $\mathbb{Z}_2\mathbb{Z}_4$ -linear codes form a wide class of \mathbb{Z}_2 -linear codes. Moreover, the equivalence between $\mathbb{Z}_2\mathbb{Z}_2[u]$ -duality and \mathbb{Z}_2 -duality (Corollary 1), suggests that $\mathbb{Z}_2\mathbb{Z}_2[u]$ -linear codes have no meaningful additional properties to those of \mathbb{Z}_2 -linear codes. However, the partition of the coordinate set into two subsets (the \mathbb{Z}_2 and the $\mathbb{Z}_2[u]$ coordinates) open some possible lines of research. In particular, cyclic $\mathbb{Z}_2\mathbb{Z}_2[u]$ -linear codes are studied in [2, 3, 14].

Another interesting point is the search for \mathbb{Z}_2 -linear non- $\mathbb{Z}_2\mathbb{Z}_2[u]$ -linear codes. In other words, the search for binary linear codes with automorphism group of odd order, according to Corollary 2.

Acknowledgements

The author thanks Prof. Josep Rifà for valuable comments on automorphism groups of linear codes.

References

1. I. Aydogdu, T. Abualrub, I. Siap, "On $\mathbb{Z}_2\mathbb{Z}_2[u]$ -additive codes," *Int. J. Comput. Math.*, vol. 9, pp. 1806-1814, 2015.
2. T. Abualrub, I. Siap and H. Aydin, " $\mathbb{Z}_2\mathbb{Z}_4$ -additive cyclic codes," *IEEE Trans. Inform. Theory*, vol. 60, pp. 1508-1514, 2014.
3. T. Abualrub, I. Siap and I. Aydogdu, " $\mathbb{Z}_2(\mathbb{Z}_2 + u\mathbb{Z}_2)$ -linear cyclic codes," In *Procs. Int. Multiconference of Engineers and Computing Science*, vol. II, 2014, Hong Kong.
4. J. Borges, C. Fernández-Córdoba, J. Pujol, J. Rifà and M. Villanueva, " $\mathbb{Z}_2\mathbb{Z}_4$ -linear codes: generator matrices and duality," *Designs, Codes and Cryptography*, vol. 54, pp. 167-179, 2010.
5. J. Borges, C. Fernández-Córdoba and R. Ten-Valls, " $\mathbb{Z}_2\mathbb{Z}_4$ -additive cyclic codes, generator polynomials and dual codes," *IEEE Trans. Inform. Theory*, vol. 62, pp. 6348-6354, 2016.
6. J. Borges and J. Rifà, "A characterization of 1-perfect additive codes," *IEEE Trans. Inform. Theory*, vol. 45, pp. 1688-1697, 1999.
7. J.H. Conway, R.T. Curtis, S.P. Norton, R.A. Parker, R.A. Wilson, *ATLAS of finite groups*, Oxford Univ. Press, 1985.
8. C. Fernández-Córdoba, J. Pujol, M. Villanueva, "Involutions in binary perfect codes," *IEEE Trans. Inform. Theory*, vol. 57, pp. 5926-5932, 2011.
9. C. Fernández-Córdoba, J. Pujol, M. Villanueva, " $\mathbb{Z}_2\mathbb{Z}_4$ -linear codes: rank and kernel," *Designs, Codes and Cryptography*, vol. 56, pp. 43-59, 2010.
10. R.E.J. Fraser, *The involutions of the Mathieu groups*, MA Thesis, Univ. of British Columbia, 1966.
11. A.R. Hammons, P.V. Kumar, A.R. Calderbank, N.J.A. Sloane and P. Solé, "The \mathbb{Z}_4 -linearity of kerdock, preparata, goethals and related codes," *IEEE Trans. on Information Theory*, vol. 40, pp. 301-319, 1994.
12. F.J. MacWilliams and N.J.A. Sloane, *The Theory of Error-Correcting Codes*, North-Holland Publishing Company, 1977.
13. J. Pujol and J. Rifà, "Translation-invariant propelinear codes," *IEEE Trans. Inform. Theory*, vol. 43, pp. 590-598, 1997.
14. B. Srinivasulu, Maheshanand Bhaintwal, " $\mathbb{Z}_2(\mathbb{Z}_2 + u\mathbb{Z}_2)$ -additive cyclic codes and their duals," *Discr. Math. Alg. App.*, vol. 8, 19 pages, 2016.